Received 26 April 2016; | Revised 6 June 2016; | Accepted 6 June 2016

DOI: xxx/xxxx

ARTICLE TYPE

Towards improved satellite telecommand link availability

Noels N.*[1] | Aguilar-Sánchez I.[2]

[1]Telecommunications and Information Processing Department, UGent, Ghent, Belgium

[2]Electrical Engineering Department, European Space Research and Technology Centre, Noordwijk, The Netherlands

Correspondence

*Noels Nele, UGent, Sint-Pietersnieuwstraat 41, B-9000 Gent, Belgium. Email: nele.noels@ugent.be

Summary

Compliant with the Consultative Committee for Space Data Systems (CCSDS) set of protocols, we explore enhancing the availability service for space links. In particular, we consider specific improved defences against jamming attacks affecting symbol synchronization. More robust adaptive closed-loop symbol synchronizers are designated with a view to the planned update of the CCSDS standard for the telecommand synchronization and channel coding sublayer of the data link layer. It is shown that adaptive schemes exploiting instantaneous jammer state information are recommended to counter destructive attacks that may harm the availability.

KEYWORDS:

Security services, space links, availability, spread spectrum

1 | INTRODUCTION

Information security measures targeting availability aim at guaranteeing reliable access to sent information by authorized parties. Due to the exposed nature of the wireless link between the ground station and the space segment, satellite telecommand (TC) systems (used for control and maintenance of the satellite) are very susceptible to jamming attacks. By simply emitting a noise-like interference signal into the frequency band of the TC system, a jammer can effectively prevent the reception of the intended signal. Loss of TC link availability due to uplink jammers that target the TC receiver of a satellite not only forms a realistic threat, it also constitutes a major security risk. If an attacker succeeds in denying the ground station to control the satellite, the success of a mission can be severely compromised.

As jamming attacks are almost impossible to prevent, the development and use of improved jamming resistant protocols is desirable. No technique will provide a 100% immunity to jamming but suitable transmission security (TRANSEC) measures in the physical layer may prevent that the TC space link can effectively be taken down by a relatively simple and inexpensive hostile emitter. For one thing, next generation TC systems will adopt cryptographic direct-sequence spread spectrum (DSSS) modulation with a very long pseudo-noise spreading code repetition period and a high spreading factor[1]. Assuming ideal circumstances, the spreading of the useful signal over a larger frequency band by means of a secret spreading code ensures that a jammer must be several times more powerful than the legitimate emitter if it wants to have a substantial impact. On the other hand, the new issue of the CCSDS satellite telecommand synchronization and channel coding sublayer protocol[2], published in september 2017, has introduced a novel communication link transmission unit (CLTU) structure with advanced LDPC channel coding. It has been shown[3,4] that, under perfect synchronization, these codes can offer an increased resilience against jamming. In practice, however, a system is never a priori synchronized and the structures that are in place to perform synchronization are themselves susceptible to jamming attacks.

The ultimate goal of an attacker is to prevent the receiver from correctly decoding the conveyed information. However, carrier synchronization, spreading code synchronization, symbol synchronization and frame synchronization are all indispensable for correct decoding. As a result, a jammer that disturbs any of the corresponding synchronization procedures beyond functionality is as effective as a jammer that is specifically designed to destroy the decoding performance. In other words, a TC receiver is only as robust against jamming attacks as its most vulnerable part. In this respect, the development of an on-board *spreading code synchronizer* capable of fast acquiring very long spreading codes at low signal-to-noise ratio and large jammer-over-signal power ratio has been an important first step[5]. A more recent study[6] has considered the impact of jamming on the performance of a candidate *frame synchronization* algorithm for TC applications. The corresponding results confirm the potential of the novel

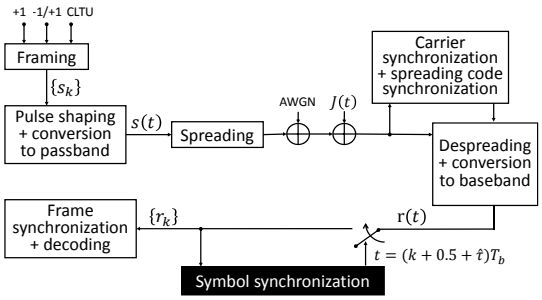

FIGURE 1 Satellite TC communication system block diagram.

CLTU structure (with multiple LDPC code blocks and a novel 64-bit start sequence [2]) as an effective protection measure against jamming. What is still missing today is an analysis of the *carrier and symbol synchronization* processes under jamming conditions.

Whereas symbol synchronization in additive white Gaussian noise (AWGN) channels is a well investigated problem, symbol synchronization in the presence of jamming has received very little attention in the literature. To fill this gap, we study symbol synchronization under jamming conditions in this work. More specifically, we analyse the effect of jamming on the performance of several closed-loop symbol synchronizers and designate more robust techniques. A jamming attack targeting symbol synchronization can impact the system performance in two ways. If the symbol timing is not timely acquired, the first couple of CLTUs of a communications session might get lost. If the symbol timing tracking error becomes too large, the communication link might be temporary deactivated due to a loss of symbol lock. This requires re-acquisition of the symbol timing and causes the loss of one or more CLTUs. For the long spreading code repetition periods envisaged for future TC applications (between 2^{20} and 2^{26} chips [5]) pulsed jamming with a well-chosen duty cycle is usually considered as the most realistic and most harmful type of jamming for all post-despreading processing [4,6]. For this reason, we focus our analysis on wideband pulsed jamming. Furthermore, carrier and spreading code synchronization, which are typically performed prior to the start of the symbol synchronization process [7], will be assumed perfect.

The paper is organized as follows. Section 2 describes the system under investigation. In Section 3, we derive a generic expression for the linearised mean squared symbol timing error (LMSTE). In Sections 4 to 6, this expression is used to assess the performance of specific synchronization structures. Numerical LMSTE results are provided and a comparison between the different techniques is performed. In Section 7 we draw conclusions.

2 | SYSTEM DESCRIPTION

The system under investigation is a satellite TC communication system using coded unit-energy Binary Phase Shift Keying (BPSK) and DSSS modulation.

The transmitting ground station and the receiving satellite adopt the protocol described in the CCSDS recommendations [2,7]. First, the ground station sends an unmodulated spreading code sequence, i.e., an all-ones symbol sequence, to allow carrier and spreading code synchronization at the satellite. As soon as the satellite acquires carrier and spreading code synchronization, the symbol timing synchronization process is initiated. Of course, symbol synchronization requires bit transitions, so the symbol timing acquisition processing only truly starts as soon as the satellite receives the symbol acquisition sequence, consisting of a continuous repetition of the (1, -1) symbol pattern. This transmission format continues until the transmission of a first CLTU, and starts again after each CLTU (for an unconstrained period of time) to keep track of the symbol timing while the transmission of a (next) CLTU is pending. A block diagram showing the relevant parts of the TC communication system is depicted in Fig. 1 . The transmitted symbol sequence $\{\mathrm{s_k}\}$ includes the all-ones symbol sequence, the alternating symbol sequences and the CLTU symbol sequences. The entire symbol sequence is converted into a sequence of non-return-to-zero pulses. This baseband signal is modulated on a sinusoidal carrier, and the resulting signal $\mathrm{s}(\mathrm{t})$ is multiplied with a pseudo noise (PN) chip sequence to accomplish the spreading operation.

During transmission, the DSSS signal is affected by AWGN with one-sided spectral density $\mathrm{N_0}$ and by a pulsed jamming signal $\mathrm{J}(\mathrm{t})$. The jammer is characterized by a sequence of inactive and active periods. The fraction of the time that the jammer is active, is referred to as the duty cycle ρ, with $0 \leq \rho \leq 1$. During inactive periods the jammer remains silent. During active periods the jammer power equals $\mathrm{P_{J,p}}$, where the subscript 'p' refers to 'peak'. By not transmitting continuously, the jammer saves power. The long-term average jammer power $\mathrm{P_{J,avg}} = \rho \mathrm{P_{J,p}}$ is only a fraction

ρ of the peak jammer power $P_{J,p}$. In the following, the jammer will be assumed to work with non-overlapping periods of Y symbol intervals long. Each period, the jammer is active during D consecutive symbol intervals and inactive during $Y - D$ symbol intervals; correspondingly, the duty cycle of the jammer equals $\rho = D/Y$. Moreover, to simplify the analysis, the boundaries of the active and inactive periods are further assumed to coincide with the symbol boundaries of the useful signal, so that a bit interval from the useful signal is either completely hit or not hit by the jammer.

The adversary is assumed to be computationally and storage bounded, such that it is not capable of recovering the employed spreading code. We further assume that the jammer is aware of all the protocol details that are known to be public. We also assume that the jammer might have the capability to sense ongoing TC activity. In that case, the jammer can save power by staying quite in-between communications sessions. As soon as it senses activity on the channel, it starts transmitting.

In the receiver, the resulting signal is first despread (assuming perfect spreading code synchronization) and then converted to baseband (assuming perfect carrier phase and frequency synchronization). Taking into account the presence of an automatic gain control unit that normalizes the level of the incoming signal, prior to further processing in the receiver, the resulting signal can be represented as:

$$r(t) = \sum_k s_k p(t - kT_b - \tau T_b) + w(t), \tag{1}$$

with $p(t) = \frac{1}{\sqrt{T_b}}$, for $t \in [0, T_b]$, and $p(t) = 0$, otherwise; τT_b denotes the unknown time delay of the symbol boundaries in the received signal vis-a-vis the local reference clock, and $w(t)$ represents the combined contribution from the AWGN and the pulsed jammer. For a variety of jammer waveforms and when the spreading factor $\frac{T_b}{T_c}$ is large[4], the jamming contribution to $w(t)$ can be modelled by a zero-mean Gaussian random process with time-dependent normalized power spectral density, i.e., $N_{0,eq}(k)/(2E_s)$ if $t \in [kT_b, (k+1)T_b]$. Here, E_s denotes the received symbol energy, which corresponds to a received signal power of $P_s = E_s/T_b$. When the jammer is active we have $N_{0,eq}(k) = N_0 + J_{0,p}$, with $J_{0,p} = P_{J,p}T_c$; when the jammer is inactive during the kth bit interval we have $N_{0,eq}(k) = N_0$. Hence, during its active periods the jammer has the same effect as AWGN with one-sided spectral density $J_{0,p}$.

The effect of T_b/T_c and ρ is illustrated in the Table below where an overview is provided of the average jammer-to-signal power ratio $P_{J,avg}/P_s = \rho(J_{0,p}/E_s)(T_b/T_c)$ that is required to obtain a $J_{0,p}$ value equal to the symbol energy E_s (i.e., $J_{0,p}/E_s$ = 0 dB[1]), for $T_b/T_c \in \{10, 100, 1000\}$[2] and $\rho \in \{0.1, 0.5, 1\}$.

J/S	$J_{0,p}/E_s$ = 0 dB		
	ρ=0.1	ρ=0.5	ρ=1
T_b/T_c=10	0 dB	7 dB	10 dB
T_b/T_c=100	10 dB	17 dB	20 dB
T_b/T_c=1000	20 dB	27 dB	30 dB

With respect to symbol synchronization we can distinguish two cases: (i) synchronous data modulation of the PN sequence and (ii) asynchronous data modulation of the PN sequence. In the first case, symbol boundaries coincide with chip boundaries and occur every $\frac{T_b}{T_c}$ chip periods. Under these circumstances symbol synchronization can be performed as follows. First, the received signal obtained after spreading and conversion to baseband is sampled at the chip rate. Then, the position of a sequence that consists of an alternation of $\frac{T_b}{T_c}$ (+1) samples and $\frac{T_b}{T_c}$ (-1) samples is located in the resulting sample sequence. In total $2\frac{T_b}{T_c}$ possible positions need to be researched. This synchronization problem shows many parallels to the frame synchronization problem investigated in[6]. In the second case, symbol transitions occur in the middle of a chip. This implies that symbol timing needs to be acquired independently from chip timings. The latter case will be considered further in this paper. To reflect the receiver's initial uncertainty about τ, we model the parameter τ in (1) as a continuous random variable with a uniform distribution over $[-0.5, 0.5]$. For $t < 0$, $r(t)$ corresponds to the all-ones symbol sequence. For time instances after $t = 0$ (and before transmission of the first CLTU) $r(t)$ corresponds to the alternating -1/+1 symbol sequence. As, strictly speaking, symbol synchronization needs to be established prior to CLTU transmission, we will ignore the presence of CLTUs in the following.

Based on the signal $r(t)$, the symbol synchronizer at the satellite produces an estimate $\hat{\tau}$ of τ. This estimate is used to locate the symbol boundaries. If a jamming attack effectively succeeds in preventing symbol timing acquisition this may result in a denial of service. As a first step in the investigation of the impact of pulsed jamming on the symbol acquisition procedure, we consider the basic discrete-time feedback timing

[1]With $J_{0,p}/E_s$ = 0 dB and assuming a nominal signal-to-thermal-noise ratio per BPSK symbol of 7 dB as in previous studies[4,6], the signal-to-noise-plus-interference ratio decreases to only -0.8 dB when the jammer is active. It has been shown[4,6] that a $J_{0,p}/E_s$ above 0 dB are likely to causes a severe performance degradation of the frame synchronization (channel decoding) subsystems, in particular if the opponent employs a pulse active period that is long as compared to the length of the start sequence (code words).

[2]For TC applications, values of T_b/T_c ranging from 10 to 1000 are envisaged.

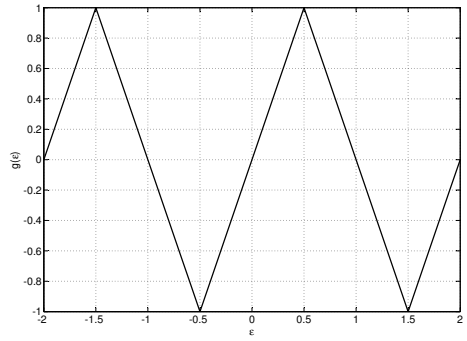

FIGURE 2 Timing error detector characteristic.

synchronizer that updates the estimate of τ once per symbol interval, according to the following recursion:

$$\hat{\tau}_{k+1} = \hat{\tau}_k + \lambda_k g_k, \tag{2}$$

with $\hat{\tau}_0 = 0$ and

$$g_k = \Re\left\{(-1)^k r_k\right\},$$

where

$$r_k = \int r(u)\, p\left(u - \left(k + \frac{1}{2} + \hat{\tau}_k\right) T_b\right) \mathrm{d}u. \tag{3}$$

This procedure requires a matched filter output sample r_k from (3) per symbol period T_b, at the decision instants $t = \left(k + \frac{1}{2} + \hat{\tau}_k\right) T_b$. The quantity λ_k in (2) is referred to as the loop gain. The value of λ_k controls the dynamics of the updating procedure. In general, fast symbol timing acquisition and a low mean square timing error (MSTE) during tracking are desirable. However, in general, these two properties are difficult to achieve simultaneously.

3 | LINEARIZED SYMBOL TIMING ACQUISITION PERFORMANCE

We compute the linearised performance of (2).

Defining the timing error during the kth symbol interval as $\epsilon_k = \tau - \hat{\tau}_k$, it is easily verified that g_k can be decomposed as the sum of its average $g(\epsilon_k)$ and a zero-mean statistical fluctuation $W_k(\epsilon_k)$, with

$$W_k(\epsilon_k) = \frac{s_k}{\sqrt{T_b}} \int_{kT_b}^{(k+1)T_b} w(t + \hat{\tau}_k + 0.5)\, \mathrm{d}t, \tag{4}$$

and

$$g_k = g(\epsilon_k) + W_k(\epsilon_k), \tag{5}$$

where $g(\epsilon)$ is commonly referred to as the timing error detector characteristic. It is a triangular wave function with period 2, amplitude 1 and $g(0.5) = 1$, demonstrating odd symmetry (as depicted in Fig. 2):

$$g(\epsilon) = 4\left|\frac{\epsilon}{2} + \frac{1}{4} - \left\lfloor \frac{\epsilon}{2} + \frac{3}{4} \right\rfloor\right| - 1. \tag{6}$$

In (6), $\lfloor x \rfloor$ denotes the largest integer smaller than or equal to x and $|x|$ denotes the absolute value of x.

Assuming small timing errors, the following linearisation of (5) applies:

$$g_k = 2\epsilon_k + W_k, \tag{7}$$

where W_k is a short-hand notation for $W_k(0)$, and $\{W_k\}$ are independently distributed Gaussian noise variables with zero mean and variance $\frac{N_{0,\mathrm{eq}}(k)}{2E_s}$. If the kth symbol period is unjammed, $N_{0,\mathrm{eq}}(k)$ equals N_0 and, if the kth symbol period is jammed, $N_{0,\mathrm{eq}}(k)$ equals $N_0 + J_{0,\mathrm{p}}$.

Substituting (7) into (2) we obtain:

$$\epsilon_{k+1} = (1 - 2\lambda_k)\,\epsilon_k - \lambda_k W_k. \tag{8}$$

Solving this equation yields for $k \geq 0$:

$$\epsilon_k = \epsilon_{1,k} + \epsilon_{2,k}, \tag{9}$$

where

$$\epsilon_{1,k} = \epsilon_0 \left[\prod_{i=0}^{k-1} (1 - 2\lambda_i) \right] \tag{10}$$

and

$$\epsilon_{2,k} = \sum_{m=0}^{k-1} \Lambda_{k,m} W_{k-m-1}, \tag{11}$$

with

$$\Lambda_{k,m} = \begin{cases} \left(\prod_{i=0}^{m-1} (1 - 2\lambda_{k-m+i}) \right) \lambda_{k-m-1} & , m \geq 1 \\ \lambda_{k-1} & , m = 0 \end{cases}. \tag{12}$$

The timing error ϵ_k consists of 2 contributions. The first contribution $\epsilon_{1,k}$ is the result of the initial timing error ϵ_0. The second contribution $\epsilon_{2,k}$ stems from the equivalent noise (noise + jamming) affecting the observation. In all practical cases the quantity $|1 - 2\lambda_k|$ is smaller than 1, so that the timing error (9) exhibits a decaying acquisition transient whose duration, for small $\{\lambda_k\}$, increases with decreasing $\{\lambda_k\}$. For large k, the timing error (9) can be safely approximated by $\epsilon_k \approx \epsilon_{T,k}$ with $\epsilon_{T,k}$ given by (11), with the upper bound on the summation index going to infinity; we have

$$\epsilon_{T,k} = \sum_{m=0}^{\infty} \Lambda_{k,m} W_{k-m-1}. \tag{13}$$

When ϵ_k starts behaving as $\epsilon_{T,k}$, the loop is said to enter *tracking mode (T)*; until then the loop is said to be in *acquisition mode*.

For given ϵ_0 and for a given location of the jammer pulses, the linearised MSTE (LMSTE) resulting from (9) is

$$\mathbb{E}\left[\epsilon_k^2\right] = \epsilon_{1,k}^2 + \mathbb{E}\left[\epsilon_{2,k}^2\right], \tag{14}$$

where $\mathbb{E}[\cdot]$ denotes averaging over the equivalent noise, conditioned on the location of the jammer pulses. In tracking mode, the timing error equals (13) which has zero mean and variance (15)

$$\mathbb{E}\left[\epsilon_{T,k}^2\right] = \sum_{m=0}^{\infty} \Lambda_{k,m}^2 \frac{N_{0,\mathrm{eq}}\,(k-m-1)}{2E_s}. \tag{15}$$

In the following, we evaluate and discuss the LMSTE performance (14) with three different loop gain selection policies under a variety of pulsed jamming conditions.

4 | CONSTANT LOOP GAIN

The conventional approach is to use a constant (CONST) loop gain, i.e., $\lambda_k = \lambda$ for all k, with λ left as the only design parameter[8]. In this case

- The coefficients $\Lambda_{k,m} = (1 - 2\lambda)^m \lambda$ in (15) depend only on m and not on k. We write $\Lambda_{k,m} = \Lambda_m$.
- For small values of λ, $\mathbb{E}\left[\epsilon_{T,k}^2\right]$ (15) behaves as the response of a first-order linear time-invariant system with time constant $\top = \frac{1}{2\lambda}$ (exponential decay constant of Λ_m) to $\frac{N_{0,eq}(k)}{2E_s}$.
- In case of no (D = 0) or continuous (D = Y) jamming, $\mathbb{E}\left[\epsilon_{T,k}^2\right]$ (15) becomes independent of k. It is easily verified that

$$\mathbb{E}\left[\epsilon_{T,k}^2\right] = \frac{\lambda}{4\,(1-\lambda)} \begin{cases} \frac{N_0}{2E_s} & , D = 0 \quad (a) \\ \frac{N_0 + J_{0,p}}{2E_s} & , D = Y \quad (b) \end{cases}, \tag{16}$$

  where the approximation $\frac{\lambda}{4(1-\lambda)} \approx \frac{\lambda}{4}$ can be applied for $\lambda \ll 1$.

Fig. 3 shows the LMSTE from (14). Here, $\epsilon_0 = 1$, $\lambda_k \equiv \lambda$ = 0.01, ρ = 0.1, E_s/N_0 = 7 dB and $E_s/(J_{0,p} + N_0)$ = -3 dB[3]; several values of the pulse period D and randomly generated jammer pulse locations are considered. We make the following observations. During acquisition, the LMSTE is not affected by the presence of jamming; this is consistent with (10). On the other hand, the behaviour of the LMSTE during tracking, i.e., $\mathbb{E}\left[\epsilon_{T,k}^2\right]$, strongly depends on the value of the jammer parameters D and Y.

[3] In previous studies, assessing the decoding and the frame synchronization performance of envisaged satellite TC communication systems under pulsed jamming conditions, for a nominal operating signal-to-noise ratio (SNR) E_s/N_0 of 7 dB, these system parts have been shown to be robust against pulsed jamming conditions corresponding to $E_s/(N_0 + J_{0,p})$ values as low as 0 dB. For the purpose of easy interpretation, in this paper, the baseline values for E_s/N_0 and $E_s/(N_0 + J_{0,p})$ are set to 7 dB and -3 dB, respectively; hence, the equivalent SNR value is exactly 10 dB lower when the jammer is active than when the jammer is inactive.

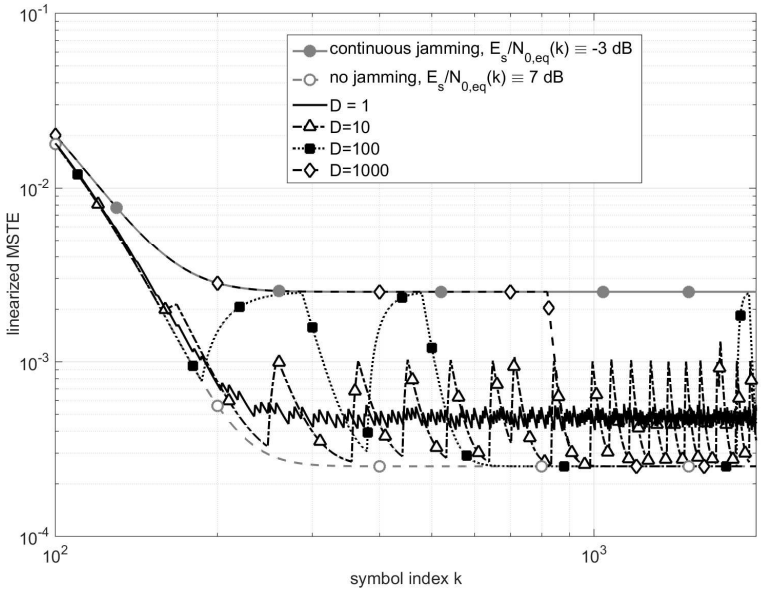

FIGURE 3 LMSTE of CONST, for E_s/N_0 = 7 dB, $E_s/(J_{0,p} + N_0)$ = -3 dB, $\epsilon_0 = 1$, $\lambda_k \equiv \lambda$ = 0.01, $\rho = 0.1$, several D and randomly generated locations of the jammer pulses.

- For D = 1, $\mathbb{E}\left[\epsilon^2_{T,k}\right]$ (15) remains significantly larger than the tracking LMSTE that would be obtained in the absence of jamming. More specifically, $\mathbb{E}\left[\epsilon^2_{T,k}\right]$ shows only small fluctuations around $\frac{\bar{N}_{0,eq}}{2E_s}\frac{\lambda}{4(1-\lambda)}$, which is the tracking mode LMSTE of the synchronization scheme when $N_{0,eq}(k)$ is replaced by its long-term time average $\bar{N}_{0,eq} = N_0 + \rho J_{0,p}$. This can be explained as follows. If D = 1, then the overall jammer period Y = 10 is small as compared to the time constant $\top$ = 50 , such that in (15) Λ_m can be considered as more or less constant over the duration of a repetition period Y. This indeed yields

$$\begin{aligned}
\mathbb{E}\left[\epsilon^2_{T,k}\right] &= \sum_{m=0}^{\infty}\sum_{m'=0}^{Y-1}\Lambda^2_{m'+mY}\frac{N_{0,eq}(k-m'-mY-1)}{2E_s},\\
&\approx \sum_{m=0}^{\infty}\Lambda^2_{mY}\left(\sum_{m'=0}^{Y-1}\frac{N_{0,eq}(k-m'-mY-1)}{2E_s}\right),\\
&\approx \frac{\bar{N}_{0,eq}}{E_s}Y\sum_{m=0}^{\infty}\Lambda^2_{mY} \approx \frac{\bar{N}_{0,eq}}{E_s}\sum_{m=0}^{\infty}\Lambda^2_{m},\\
&= \frac{\bar{N}_{0,eq}}{2E_s}\frac{\lambda}{4(1-\lambda)}.
\end{aligned}$$

- For D = 10, $\mathbb{E}\left[\epsilon^2_{T,k}\right]$ switches between the tracking LMSTE that would be obtained in the absence of jamming (16(a)) and a larger value that is strictly smaller than the tracking LMSTE that would be obtained in the presence of continuous jamming with $J_0 = J_{0,p}$ (16(b)). In this case, D = 10 is small as compared to the time constant $\top$ = 50 but (Y − D) = 90 is not. As a result, the effect on $\mathbb{E}\left[\epsilon^2_{T,k}\right]$ of the low $N_{0,eq}(k)$ values that precede a jamming pulse remains in play for longer than that pulse's duration, whereas the effect of one jamming pulse is likely to have completely disappeared before the next one arrives.

- For D = 100 and D = 1000, the tracking LMSTE switches between the tracking LMSTE that would be obtained in the absence of jamming (16(a)) and the tracking LMSTE that would be obtained in the presence of continuous jamming with $J_0 = J_{0,p}$ (16(b)), with transients having a duration in the order of the time constant $\top$ = 50. Since, D and (Y − D) are both large as compared to T, a steady state regime is achieved, both during and in between jammer pulses.

In all cases, the tracking LMSTE is lower than or equal to the tracking LMSTE that would be obtained in the presence of continuous jamming with $J_0 = J_{0,p}$ (16(b)). This indicates that a synchronizer with loop gain λ_J is capable of guaranteeing the same maximum tracking error variance in the presence of pulsed jamming as a synchronizer with loop gain λ in the absence of jamming, provided that λ_J is selected $\frac{N_0+J_{0,p}}{N_0}$ times smaller than λ. Unfortunately, this design will also increase the time constant of the loop with a factor $\frac{N_0+J_{0,p}}{N_0}$, which results in a prolonged acquisition transient

and reduced ability to follow variations of τ over time. To avoid that the lower acquisition speed results in the loss of CLTUs (which happens if symbol synchronization is not acquired in time for the reception of the first CLTU), the length of the symbol acquisition sequence can be increased by a factor $\frac{\lambda}{\lambda_J}$.

Hence, the impact of jamming on the CONST symbol synchronization process can be effectively mitigated by decreasing the loop gain and proportionally increasing the allowed acquisition time. However, this approach also has important disadvantages. First, the transmitter needs to send a longer symbol acquisition sequence. This needs to be done in every communications session and therefore causes a considerable amount of additional overhead. Second, the system is not flexible and in that sense ill-adjusted to pulsed jamming attacks. The loop gain is dimensioned for some maximum peak jamming power and kept fixed over time. So, on the one hand the system is not armed against attacks with a larger than expected peak power. On the other hand, the loop's tracking capability is unnecessary low during the periods without jamming activity (which, with pulsed jamming, can be the case during a large percentage of the time).

In the next section, we try to resolve these issues by proposing adaptive synchronizer structures with time-varying loop gains that better account for the presence of pulsed jamming. Perfect knowledge of the quantities $N_{0,\mathrm{eq}}(l)$ will be assumed. In practice, the exact values of $N_{0,\mathrm{eq}}(l)$ are not available and estimates $\hat{N}_{0,\mathrm{eq}}(l)$ obtained from $r(t)$ need to be used in stead. Nevertheless, the performance of a synchronizer with perfect $N_{0,\mathrm{eq}}(l)$ values, serves as a useful benchmark for such practical symbol synchronizers.

5 | PIECEWISE CONSTANT LOOP GAIN

As a first approach, we propose to select λ_k such that, at each time instant k, we have

$$\lambda_k = \lambda \frac{N_0}{N_{0,\mathrm{eq}}(k)}, \tag{17}$$

which is proportional to a single design parameter λ as well as inversely proportional to the instantaneous value of $N_{0,\mathrm{eq}}(k)$. Under pulsed jamming conditions, the loop gain becomes a piecewise constant (PW_CONST) function of the time index k with λ_k equal to λ, if the kth symbol interval is not jammed and to $\lambda_J = \lambda \frac{N_0}{N_0 + J_{0,p}}$, otherwise.

Let us assume that the jammer state (active or inactive) remains unaltered during the symbol periods $k-1, k-2, \ldots, k-L_k-2$ and a jammer state transition (from active to inactive, or vice versa) occurs between the symbol period $k-L_k-2$ and $k-L_k-1$. Then, substituting (17) into (15) yields

$$\begin{aligned}
&\mathbb{E}\left[\epsilon_{T,k}^2\right] \\
&= \frac{\lambda N_0}{2E_s} \sum_{m=0}^{\infty} \frac{\Lambda_{k,m}^2}{\lambda_{k-m-1}}, \\
&= \frac{\lambda N_0}{2E_s} \left(s_{k-1,L_k} + f_{k-1,L_k}\left(\rho S_J + (1-\rho) S\right)\right), \\
&\approx \frac{\lambda N_0}{8E_s},
\end{aligned} \tag{18}$$

with

$$\begin{aligned}
f_{k,l} &= (1-2\lambda_k)^{2l}, \\
s_{k,l} &= \sum_{m=0}^{l-1} f_{k,m}\lambda_k = \frac{1-f_{k,l}}{1-f_{k,1}}\lambda_k = \frac{1-f_{k,l}}{4(1-\lambda_k)}, \\
S_J &= \sum_{m=0}^{\infty} (1-2\lambda_J)^{2m}\lambda_J = \frac{1}{4(1-\lambda_J)}, \\
S &= \sum_{m=0}^{\infty} (1-2\lambda)^{2m}\lambda = \frac{1}{4(1-\lambda)}.
\end{aligned}$$

The approximation (18) holds provided that λ_k is much smaller than 1 for all k; in that case, PW_CONST yields a $\mathbb{E}\left[\epsilon_{T,k}^2\right]$ that is independent of the location of the jammer pulses.

Fig. 4 (for $D = 10^4$) and Fig. 5 (for $D = 100$) compare the linearised MSTE resulting from (9) for $\lambda_k = \lambda \frac{N_0}{N_{0,\mathrm{eq}}(k)}$ (PW_CONST) and $\lambda_k = \lambda$ (CONST); we assume $\epsilon_0 = 1$, λ = 0.01 and $\rho = 0.1$. In both figures, results are presented for 3 different, randomly generated, jammer pulse locations (sim_1, sim_2, sim_3). For each set of jammer pulse locations (each sim), the linearised MSTE of both receivers is evaluated. Again, we assume a jamming scenario with ρ = 0.1, E_s/N_0 = 7 dB and $E_s/(J_{0,p} + N_0)$ = -3 dB. Our results show that, as compared to a loop with a constant loop gain, the approach with a piecewise constant loop gain according to (17) yields

1. A lower tracking LMSTE during the active periods of the jammer.

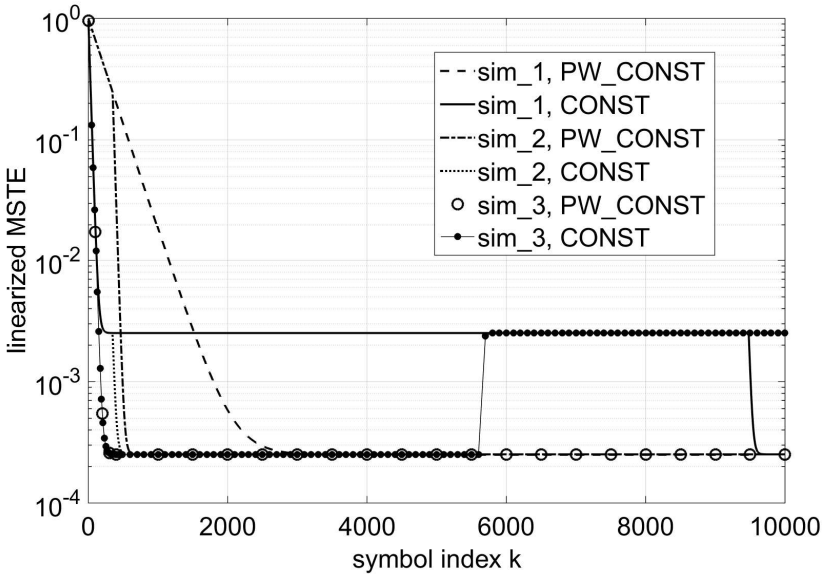

FIGURE 4 Linearized MSTE with $\lambda_k = \lambda \frac{N_0}{N_{0,eq}(k)}$ (PW_CONST) and $\lambda_k = \lambda$ (CONST), for $k \geq 0$ assuming E_s/N_0 = 7 dB, $E_s/(J_{0,p} + N_0)$ = -3 dB, $\epsilon_0 = 1$, λ = 0.01, $\rho = 0.1$, $D = 10^4$ and two randomly generated sets of jammer pulse locations (sim_1 and sim_2, respectively) are considered.

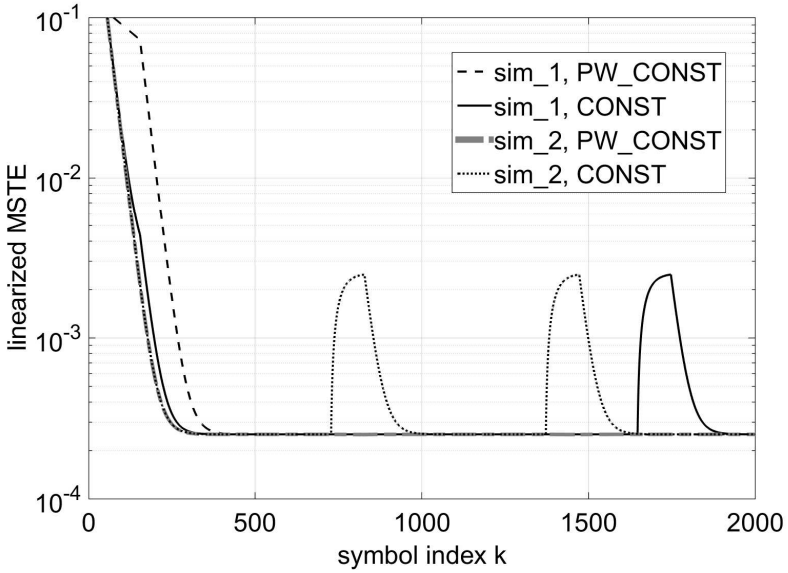

FIGURE 5 Linearised MSTE with $\lambda_k = \lambda \frac{N_0}{N_{0,eq}(k)}$ (PW_CONST) and $\lambda_k = \lambda$ (CONST), for $k \geq 0$ assuming $\epsilon_0 = 1$, λ = 0.01, $\rho = 0.1$, $D = 100$ and two randomly generated sets of jammer pulse locations (sim_1 and sim_2, respectively) are considered.

2. An increased acquisition period, in case of jammer activity during acquisition.

The latter observation results immediately from the fact that when a jammer pulse is detected, the loop gain is set to a lower value ($\lambda_J \leq \lambda$) and therefore the loop will react slower to time variations of τ.

The major advantage of PW_CONST as compared to CONST is that the loop gain is only decreased for a fraction ρ of the time, i.e., during the periods of jammer activity (while the original loop gain can be maintained during normal link operation). Moreover, as the loop gain's value is adapted

on the fly, the system can flexibly adjust to the instantaneous jammer peak power value without constraints. As very high peak power values are usually maintained for very short periods of time only the problem of a (temporarily) very reduced tracking capability is not that large. On the other hand, to make sure that the loop acquires the symbol timing prior to the reception of the first CLTU of a communications session, with PW_CONST just as with CONST, the length of the symbol acquisition sequence needs to be increased. If (not only the receiver but also) the transmitter has jammer state information, the length of the symbol acquisition sequence can be flexibly adjusted to the presence of jamming activity; if not the length of the symbol acquisition sequence needs to be dimensioned for some minimum loop gain. A possible approach to circumvent the decreased acquisition speed of PW_CONST, is to use CONST with $\lambda_k \equiv \lambda$ during acquisition, after which PW_CONST with λ_k from (17) is employed during tracking. An alternative approach is considered next.

6 | ADAPTIVE LOOP GAIN BASED ON KALMAN FILTERING TECHNIQUES

Optimal instantaneous loop gains can be derived from the Kalman filtering framework ([9,10] and more recently [11,12]). We obtain:

$$\lambda_k = \frac{2\hat{\sigma}_k^2}{4\hat{\sigma}_k^2 + \frac{N_{0,\mathrm{eq}}(k)}{2E_s}}, \tag{19}$$

with $\hat{\sigma}_k^2$ recursively computed according to:

$$\hat{\sigma}_k^2 = \hat{\sigma}_{k-1}^2 (1 - 2\lambda_k) + \upsilon_k^2, \tag{20}$$

where υ_k^2 is a measure for the statistical time-variability of τ. In contrast to the case where λ_k is simply adjusted to the instantaneous equivalent noise level according to (17), λ_k from (19) is not inversely proportional to $N_{0,\mathrm{eq}}(k)$. It is common practice to define the initial value $\hat{\sigma}_0^2$ of $\hat{\sigma}_k^2$ equal to 1/12, which corresponds to the variance of a timing that is uniformly distributed in $[-0.5, 0.5]$. When υ_k^2 is set to 0, both λ_k and $\hat{\sigma}_k^2$ will continuously decrease. To guarantee a certain level of tracking (and to allow a meaningful comparison with CONST and PW_CONST), one could use $\upsilon_k^2 = 0$ in (20) but replace (19) by:

$$\lambda_k = \max\left(\lambda \frac{N_0}{N_{0,\mathrm{eq}}(k)}, \frac{2\hat{\sigma}_{k-1}^2}{4\hat{\sigma}_{k-1}^2 + \frac{N_{0,\mathrm{eq}}(k)}{2E_s}}\right), \tag{21}$$

where λ again is a design parameter. The synchronizer using (21) will be further denoted as KAL_1. Under normal tracking conditions, $\lambda_k = \lambda \frac{N_0}{N_{0,\mathrm{eq}}(k)}$ as for PW_CONST such that the tracking LMSTE is again given by (18). Alternatively, υ_k^2 in (20) can be selected equal to $\lambda^2 \frac{N_0}{2E_s}$, such that, under normal tracking conditions, where $\hat{\sigma}_k^2 \to \frac{\upsilon_k^2}{2\lambda_k}$ and $4\hat{\sigma}_k^2 \ll \frac{N_{0,\mathrm{eq}}(k)}{2E_s}$, we have a loop gain $\lambda_k \approx \lambda\sqrt{\frac{N_0}{N_{0,\mathrm{eq}(k)}}}$ (yielding $\lambda_k \approx \lambda$ in the absence of jamming and $\lambda_k \approx \lambda\sqrt{\frac{N_0}{N_0+J_{0,\mathrm{p}}}} > \lambda_J$ during jammer pulses); the synchronizer using (19)-(20) with $\upsilon_k^2 = \lambda^2 \frac{N_0}{2E_s}$ will be further denoted as KAL_2.

Fig. 6 shows for $D = 100$, $\rho = 0.1$, E_s/N_0 = 7 dB and $E_s/(J_{0,\mathrm{p}} + N_0)$ = -3 dB, assuming $\epsilon_0 = 1$ and fixed randomly generated jammer pulse positions (with a first pulse occurring during acquisition), the linearised MSTE corresponding to (9) for CONST, PW_CONST, KAL_1 and KAL_2, with $\lambda = 0.01$. We observe that KAL_1 and KAL_2 acquire the symbol timing significantly faster than CONST and PW_CONST. We also see that KAL_1 yields the same tracking LMSTE as PW_CONST. This was to be expected since both loops use the same loop gain values when in tracking mode. KAL_1 and KAL_2 behave similar in the absence of jamming but KAL_2 exhibits a larger LMSTE than KAL_1 during the periods of jamming activity. This is a direct consequence of the fact that KAL_2 is by definition dimensioned to use a larger instantaneous loop gain than KAL_1 during these periods. In spite of the (limited) increases in LMSTE as compared to KAL_1, it may be concluded that KAL_2 is as an excellent candidate for making symbol synchronization robust against pulsed jamming attacks and thereby guaranteeing availability. After all, a larger loop gain not only comes with a larger tracking LMSTE, but also with a faster response to potential symbol timing variations (an aspect that is not modelled in (1)).

7 | CONCLUSIONS

In this paper, we have worked on increased robustness to pulsed jamming attacks affecting symbol synchronization. This work is relevant for the next generation CCSDS standard for satellite TC systems that is being developed with a view to improving the availability service for space links by increasing the resilience against jamming by a malicious interferer.

Assuming the presence of an alternating +1/-1 symbol acquisition sequence, we have performed a preliminary study on the performance of symbol timing acquisition procedures under pulsed jamming conditions. We have shown that the effect of (pulsed) jamming on the symbol synchronization process can be effectively mitigated by decreasing the loop gain and proportionally increasing the allowed acquisition time. Moreover, we have shown that, if the receiver has accurate instantaneous jammer state information, adaptive feedback synchronization loops with a time-variable loop gain are preferable in terms of acquisition speed, flexibility and tracking capability. Different loop gain selection methods have been

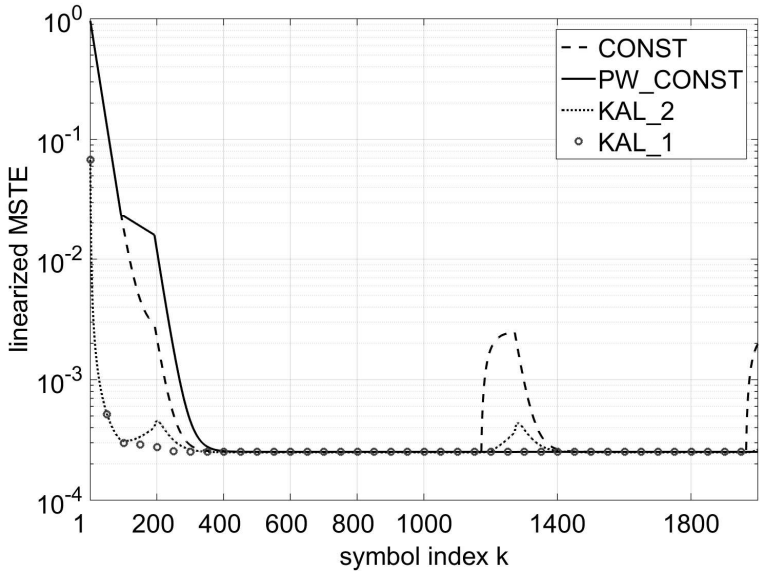

FIGURE 6 Linearised MSTE for CONST, PW_CONST, KAL_1 and KAL_2, for E_s/N_0 = 7 dB, $E_s/(J_{0,p} + N_0)$ = -3 dB, $\epsilon_0 = 1$, $\rho = 0.1$, $\lambda = 0.01$, $D = 100$ and fixed randomly generated jammer pulse positions.

compared. Each of them is characterized by a single design parameter λ. It was demonstrated that the adaptive feedback symbol timing synchronization loops KAL_1 and KAL_2, derived from the Kalman filtering framework, can provide significant protection against jamming attacks, threatening availability.

References

1. D. Fisher, I. Aguilar-Sáchez, B. Saba, G. Moury, B- Bailey, H- Weiss, M- Pilgram, D. Richter. Towards completion of the CCSDS space data link security protocol. *Proc. AIAA Conference*, 2015.

2. *TC Synchronization and Channel Coding*. CCSDS. 231.0-B-3 Blue Book. Sep. 2017.

3. P. Martinelli, E. Cianca and L. Simone, Comparison of channel codes in presence of pulsed jammers in TT&C links. *Proc. 7th Advanced Satellite Multimedia Systems Conf. and 13th Signal Processing for Space Commun. Workshop (ASMS/SPSC)*. Sep. 2014. 170-173.

4. M. Baldi, F. Chiaraluce, R. Garello, N. Maturo, I. Aguilar Sanchez and S. Cioni, Analysis and performance evaluation of new coding options for space telecommand links–part II: jamming channels. *Wiley Online Library Int. J. Satellite Commun. and Networking*. 2015. 33(6). 527-542.

5. L. Simone, G. Fittipaldi and I. Aguilar Sanchez. Fast acquisition techniques for very long PN codes for on-board secure TTC transponders. *Proc. IEEE Military Commun. Conf. (MILCOM)*. 2011. 1748-1753.

6. N. Noels and M. Moeneclaey. Performance of advanced telecommand frame synchronizer under pulsed jamming conditions. *Proc. IEEE International Conference on Communications*. 2017.

7. *TC Synchronization and Channel Coding - Summary of Concept and Rationale*. CCSDS. 230.1-G-2 Green Book. Nov. 2012.

8. N. Noels, H. Steendam and M. Moeneclaey, Performance analysis of ML-based feedback carrier phase synchronizers for coded signals. *IEEE Transactions on Signal Processing*. 2007. 55(3). 1129-1136.

9. P. F. Driessen, DPLL bit synchronizer with rapid acquisition using adaptive Kalman filtering techniques. *IEEE Transactions on Communications*. 1994. 42(9). 2673-2675.

10. B. Chun, S. H. Chois and B. Kim, A digital phase-locked loop with variable loop gains derived from RLS method. *Proc. IEEE International Conf. on Commun.*. 1997. 11-15.

11. J.-H. Won and B. Eissfeller, A tuning method based on signal-to-noise power ratio for adaptive PLL and its relationship with equivalent noise bandwidth. *IEEE Communications Letters*. 2013. 17(2). 393-396.

12. J.-H. Won, A novel adaptive digital phase-lock-loop for modern digital GNSS receivers. *IEEE Communications Letters*. 2014. 18(1). 46-49.

How to cite this article: N. Noels,and I. Aguilar-Sanchez (2017), Towards improved satellite telecommand link availability., *Int. J. Sat. Commun. Networking*, *2017;00:1–6*.